The invention claimed is:

1. A method comprising:

performing, at a client, to outgoing packets having the client's private source IP address and generalized port number (GPN) and a protocol not directly supported by a network address translator (NAT) at which the client's private source IP address and GPN are translated to a NAT's global source IP address and GPN, respectively, the functions of an Application Layer Gateway (ALG) that need to be implemented in association with the NAT's translations.

2. A method comprising:

performing, at a client, to incoming packets sent to a network address translator's (NAT's) global destination IP address and generalized port number (GPN) and having a protocol not directly supported by the NAT at which the NAT's global destination IP address and GPN are translated to the client's private destination IP address and GPN, respectively, the functions of an Application Layer Gateway (ALG) that need to be implemented in association with the NAT's translations.

3. A method comprising:

modifying, at a client, outgoing packets having the client's private source IP address and generalized port number (GPN) and a protocol not directly supported by a network address translator (NAT) at which the client's private source IP address and GPN are translated to the NAT's global source IP address and GPN, respectively, the packets being modified so as to pre-compensate for the effects on the packets of the IP address and GPN translations.

4. The method of claim 3 wherein modifying the packets comprises modifying a TCP or UDP checksum in a packet's TCP or UDP header to account for the IP address and TCP or UDP source port number translations.

5. The method of claim 4 wherein modifying the checksum comprises adding to the TCP or UDP checksum the difference between the global and private source IP addresses, and the difference between global and private TCP or UDP source port numbers.

6. The method of claim 3 wherein the protocol is an authenticating and/or encrypting-decrypting AH or ESP IPSec security protocol in a tunnel or a transport mode, and modifying the packets comprises:

before authentication and/or encryption, in the transport mode, replacing the client's source port number with a global port number, or in the tunnel mode, replacing an encapsulated client's source IP address and port number by the NAT's global IP address and port number; and

adding to a TCP or UDP checksum in a packet's TCP or UDP header, the difference between the global and private source IP addresses, and the difference between global and private TCP or UDP source port numbers.

7. The method of claim 6 further comprising processing any necessary Application Layer Protocol (ALG).

8. The method of claim 7 further comprising, for the AH protocol, computing each packet's authentication data as if the source IP address were equal to the NAT's global IP address.

9. A method comprising:

modifying, at a client, incoming packets sent to a network address translator's (NAT's) global destination IP address and generalized port number (GPN) and having a protocol not directly supported by the NAT at which the NAT's global destination IP address and GPN are translated to the client's private destination IP address and GPN, the packets being modified so as to post-compensate for the effects on the packets of the IP address and GPN translations.

10. The method of claim 9 wherein modifying the packets comprises modifying a TCP or UDP checksum in a packet's TCP or UDP header to account for the destination IP address and TCP or UDP destination port number translations.

11. The method of claim 10 wherein modifying the checksum comprises subtracting from the TCP or UDP checksum the difference between the global and private destination IP addresses, and the difference between the global and private TCP or UDP destination port numbers.

12. The method of claim 9 wherein the protocol is an authenticating and/or encrypting-decrypting AH or ESP IPSec security protocol in a tunnel or a transport mode, and modifying the packets comprises:

after authentication and/or decryption, in the transport mode, replacing the NAT's global destination port number with the client's private port number, or in the tunnel mode, replacing in a decapsulated packet the NAT's global destination IP address and port number by the client's private IP address and port number; and

subtracting from a TCP or UDP checksum in a TCP or UDP header, the difference between the global and private destination IP addresses, and the difference between the global and private TCP or UDP destination port numbers.

13. The method of claim 12 further comprising processing any necessary Application Layer Gateway (ALG) after authentication and/or decryption.

14. The method of claim 13 further comprising, for the AH protocol, computing each packet's authentication data as if the destination IP address were equal to the NAT's global IP address.

15. Apparatus at a client comprising:

means for modifying packets having the client's private source IP address and generalized port number (GPN) and having a protocol not directly supported

by a network address translator (NAT) at which the client's private source IP address and GPN are translated to the NAT's global source IP address and GPN, respectively, so as to pre-compensate for the effects on the packets of the IP address and GPN translations; and

means for sending the packets to the NAT.

16. The apparatus in accordance with claim 15 wherein the modifying means comprises means for modifying a TCP or UDP checksum in a TCP or UDP header in the packets to account for the IP address and TCP or UDP source port number translations.

17. The apparatus in accordance with claim 16 wherein the means for modifying a TCP or UDP checksum comprises means for adding to the TCP or UDP checksum the difference between the global and private source IP addresses, and the difference between global and private TCP or UDP source port numbers.

18. The apparatus of claim 15 wherein the protocol is an authenticating and/or encrypting-decrypting AH or ESP IPSec security protocol in a tunnel or a transport mode, and the means for modifying the packets comprises:

means for, before authentication and/or encryption, in the transport mode, replacing the client's source port number with a global port number, or in the tunnel mode, replacing an encapsulated client's source IP address and port number by the NAT's global IP address and port number; and

means for adding to a TCP or UDP checksum in a packet's TCP or UDP header, the difference between the global and private source IP addresses, and the difference between global and private TCP or UDP source port numbers.

19. The apparatus of claim 18 further comprising means for processing any necessary Application Layer Protocol (ALG).

20. The apparatus of claim 19 further comprising means for computing each packet's authentication data as if the source IP address were equal to the NAT's global IP address, for the AH protocol.

21. Apparatus at a client comprising:

means for receiving packets sent to a network address translator's (NAT's) global destination IP address and generalized port number and having a protocol not directly supported by the NAT at which the NAT's global destination IP address and GPN are translated to the client's private destination IP address and GPN, respectively; and

means for modifying the packets so as to post-compensate for the effects on the packets of the IP address GPN translations.

22. The apparatus of claim 21 wherein the modifying means comprises means for modifying a TCP or UDP checksum in a TCP or UDP header in the packets to account for the destination IP address and TCP or UDP destination port number translations.

23. The apparatus of claim 22 wherein the means for modifying a TCP or UDP checksum comprises means for subtracting from the TCP or UDP checksum the difference between the global and private destination IP addresses, and the difference between global and private TCP or UDP destination port numbers.

24. The apparatus of claim 21 wherein the protocol is an authenticating and/or encrypting-decrypting AH or ESP IPSec security protocol in a tunnel or a transport mode, and the means for modifying the packets comprises:

means for, after authentication and/or decryption, in the transport mode, replacing the NAT's global destination port number with the client's private port number, or in the tunnel mode, replacing in a decapsulated packet the NAT's

global destination IP address and port number by the client's private IP address and port number; and

means for subtracting from a TCP or UDP checksum in a TCP or UDP header, the difference between the global and private destination IP addresses, and the difference between the global and private TCP or UDP destination port numbers.

25. The apparatus of claim 24 further comprising means for processing any necessary Application Layer Protocol (ALG).

26. The apparatus of claim 25 further comprising means for computing each packet's authentication data as if the destination IP address were equal to the NAT's global IP address, for the AH protocol.

27. Apparatus at a client comprising:

means for performing the functions of an Application Layer Gateway (ALG) that need to be implemented in conjunction with a network address translator's (NAT's) translation of packets that are not directly supported by the NAT at which the client's private source IP address and generalized port number (GPN) are translated to the NAT's global IP address and GPN; and

means for sending the packets on which the functions of the ALG have been performed to the NAT.

28. Apparatus at a client comprising:

means for receiving packets sent to a network address translator's (NAT's) global destination IP address and generalized port number (GPN) and having a protocol not directly supported by the NAT at which the NAT's global destination IP address and GPN are translated to the client's private destination IP address and GPN, respectively; and

means for performing the functions of an Application Layer Gateway (ALG) that need to be implemented in association with the NAT's translations.

29. A computer readable media tangibly embodying a program of instructions executable by a computer to perform a method at a client, the method comprising:

modifying outgoing packets having the client's private source IP address and generalized port number (GPN) and a protocol not directly supported by a network address translator (NAT) at which the client's private source IP address and GPN are translated to the NAT's global source IP address and GPN, respectively, the packets being modified so as to pre-compensate for the effects on the packets of the IP address and GPN translations.

30. The media of claim 29 where in the method modifying the packets comprises modifying a TCP or UDP checksum in a packet's TCP or UDP header to account for the IP address and TCP or UDP source port number translations.

31. The media of claim 29 where in the method modifying the checksum comprises adding to the TCP or UDP checksum the difference between the global and private source IP addresses, and the difference between global and private TCP or UDP source port numbers.

32. The media of claim 29 where in the method the protocol is an authenticating and/or encrypting-decrypting AH or ESP IPSec security protocol in a tunnel or a transport mode, and modifying the packets comprises:

before authentication and/or encryption, in the transport mode, replacing the client's source port number with a global port number, or in the tunnel mode, replacing an encapsulated client's source IP address and port number by the NAT's global IP address and port number; and

adding to a TCP or UDP checksum in a packet's TCP or UDP header, the difference between the global and private source IP addresses, and the difference between global and private TCP or UDP source port numbers.

33. The media of claim 29 wherein the method further comprises processing any necessary Application Layer Protocol (ALG).

34. The media of claim 33 wherein the method further comprises, for the AH protocol, computing each packet's authentication data as if the source IP address were equal to the NAT's global IP address.

35. A computer readable media tangibly embodying a program of instructions executable by a computer to perform a method at a client, the method comprising:

modifying incoming packets sent to a network address translator's (NAT's) global destination IP address and generalized port number (GPN) and having a protocol not directly supported by the NAT at which the NAT's global destination IP address and GPN are translated to the client's private destination IP address and GPN, the packets being modified so as to post-compensate for the effects on the packets of the IP address and GPN translations.

36. The media of claim 35 where in the method modifying the packets comprises modifying a TCP or UDP checksum in a packet's TCP or UDP header to account for the destination IP address and TCP or UDP destination port number translations.

37. The media of claim 36 where in the method modifying the checksum comprises subtracting from the TCP or UDP checksum the difference between the global and private destination IP addresses, and the difference between the global and private TCP or UDP destination port numbers.

38. The media of claim 35 where in the method the protocol is an authenticating and/or encrypting-decrypting AH or ESP IPSec security protocol in a tunnel or a transport mode, and modifying the packets comprises:

after authentication and/or decryption, in the transport mode, replacing the NAT's global destination port number with the client's private port number, or in

the tunnel mode, replacing in a decapsulated packet the NAT's global destination IP address and port number by the client's private IP address and port number; and

subtracting from a TCP or UDP checksum in a TCP or UDP header, the difference between the global and private destination IP addresses, and the difference between the global and private TCP or UDP destination port numbers.

39. The media of claim 38 wherein the method further comprises processing any necessary Application Layer Gateway (ALG) after authentication and/or decryption.

40. The media of claim 39 wherein the method further comprises, for the AH protocol, computing each packet's authentication data as if the destination IP address were equal to the NAT's global IP address.